Privacy and Security Standards Workgroup
Draft Transcript
February 11, 2011

Presentation

Judy Sparrow – Office of the National Coordinator – Executive Director
Good afternoon, everybody, and welcome to the Privacy and Security Standards Workgroup. This is a Federal Advisory Committee, so there will be opportunity at the end of the call for the public to make comments. The call will run from 1:00 p.m. to 3:30 p.m. Eastern Time. A reminder to workgroup members, to please identify yourselves when speaking.

Let me do a quick roll call. Dixie Baker?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Walter Suarez?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Anne Castro couldn't make it. Steve Findlay? Dave McCallie?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Wes Rishel? Sharon Terry also could not make it. Steve Ondra?

Stephen Ondra – NeHC – Senior Policy Advisor
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Joy Pritts? Mike Davis?

Mike Davis – Veterans Affairs
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
John Moehrke?

John Moehrke – Interoperability & Security, GE – Principal Engineer
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Sue McAndrew? Ed Larsen? Kevin Stein?

Kevin Stein

Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Arien Malec?

Arien Malec – ONC
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Rich Kernan?

Rich Kernan – Deloitte Consulting – Health IT Specialist
Here.

Judy Sparrow – Office of the National Coordinator – Executive Director
Did I leave anyone off? With that, I'll turn it over to Dixie.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you all for dialing in. We have a number of guest speakers today, so I'd start off by thanking you all for participating. I want to begin by introducing a new workgroup member, Mike Davis, who's also one of our speakers today. Mike Davis is from the VA, and I worked with Mike for more years than either of us probably wants to admit, and I know that he will bring real value to our workgroup. So, Mike, my sincere thanks to you and to the VA for allowing us to make you a member of our workgroup. We really appreciate it.

I also want to put today's discussion into context, and this is the second item on our agenda. The role of the Privacy and Security Workgroup and indeed all of the workgroups and the entire Health Information Technology Standards Committee is changing somewhat with the startup of the full operations of the Standards and Interoperability, or S&I framework, and Arien can maybe talk a little bit about this in his presentation. I know that our HIT Standards Committee will talk more about that at our meeting next week. But now that we have some real paid for people working on standards the role of the Standards Committee is going to evolve into one of more providing up front guidance and criteria and guidance along the way and feedback, rather than us going about really directly recommending standards and doing all the back office work, if you will, ourselves. Nonetheless, the inputs that we're receiving today with respect to digital signatures I know will help inform the S&I framework and Arien's work and the ONC's work in this area. So I know that this will be useful and will help us provide feedback with respect to the S&I framework recommendations.

We have three speakers today. Our agenda is going to start with Walter reviewing the initial call on digital certificates. I think I said digital signatures. I meant digital certificates. He will review our initial call on digital certificates and the action items that we had from that call and then we're going to have three speakers. Arien Malec from the Office of the National Coordinator will be talking about the Direct Project and how digital certificates played a part, and will play a part in the Direct Project. Then Mike Davis will talk about digital certificates and how they're used with the VA health system. Finally, Rich Kernan will talk about the Nationwide Health Information Network Exchange specs for digital certificates.

With that, Walter?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Great, thank you, Dixie, and good afternoon, everyone. I also want to add my thanks to all of the speakers for being so gracious to take time today to talk to us about this, and doing so in such a very short notice is just incredible to be able to count on all of you for this to happen today.

I want to start, and I think we can move to the next slide, we're going to be switching a little bit of presentations, so if we can move to that slide, the agenda. Dixie already covered this, so I'm going to go to the next slide and talk about—and she already talked about this role. Dixie, do you want to say a few words about the role that we will probably have with respect to provider directories in the context of these new relationships with the S&I framework?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think it's very similar. The new role will really take effect with the digital certificates that will include the provider directories as well. And it will be one of recommending specifics such as, and it will be ... the full Standards Committee next week most likely will be one of defining use cases and really specifying criteria for success, if you will, and then monitoring the S&I framework work along the line and providing feedback into that group. The S&I framework team considers the Direct Project as sort of a work example that they're now tweaking moving forward. As you know, the Standards Committee did do two technical assessments of the Direct Project along the way, so it will be similar to that, although I believe the Standards Committee will have more up front input in the long run. But Arien, would you like to say a little bit more about that?

Arien Malec – ONC
Yes, thank you. I would be happy to. I think everyone recognizes in the Direct Project that we, with regard to both the Standards and the Policy Committees we didn't have the appropriate level of coordination up front. I think one of the things we want to make sure that we do in the Standards and Interoperability framework is make sure that we have the right level of coordination. As Dixie mentioned, the Standards Committee is a legislatively mandated role in recommending standards implementation specifications and certification criteria to the secretary. So by any definition the Standards Committee has a key role in the evaluation of any proposals in those areas. Where the Standards and Interoperability framework, I think, can be useful is in areas where there is nascent consensus but not actively stated consensus. That is, there's consensus that there's a problem that needs a generalized solution, there's some potential proposals for that to solve that problem, and we need the community to coalesce around one of those and coalesce around the details that will guide, for example, certification of certified EHR technologies.

In that model, the S&I framework model is to hand the work back to the Standards Committee at the end, to evaluate and make recommendations to the secretary. Because of that, it's incredibly important that up front we establish the evaluation criteria, the requirements, if you will, for the S&I work in a way that gives us a good mandate, gives us good guidance on what a solution looks like. But also in a way that allows a community to form and considerable multiple alternatives to come up with a solution that we then proposed back to the Standards Committee. In general what we're trying to get to in the revised S&I framework is a process where the Standards Committee is setting strategic direction and evaluation and is working with the S&I framework to make sure that we're essentially the operational arm working against the strategic direction and evaluation criteria, forming a community around the problem domain or challenge domain, and coming up with a solution that's grounded in that set of evaluation criteria and requirements that we can then hand back to the Standards Committee.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That's great, Arien. Basically, to emphasize, I think the bottom line is we at the Standards Committee will be providing at least three—this is going to be very much an iterative process between the Standards Committee, the S&I framework will be mentioned. We will provide some up front guidance and evaluation criteria for the S&I framework to go and implement the framework itself and do the nitty-gritty work, if you will. During that process we will also have a second role, which probably will be, as I see it, work with the S&I framework to clarify any guidance or to receive reports periodically, as I think Dixie mentioned. Then the third role really is at the end of the process when the S&I framework completes its work of implementing this framework on this particular task or this particular domain, like digital certificates or provider directories or the other ones that are coming up. At the end of that process then that role would be receiving back from the S&I framework the recommended standards after the whole evaluation

process happened and ultimately having the responsibility to provide the recommendations back to the Office of the National Coordinator. I see those three as the most significant roles of the HIT Standards Committee.

I don't know if there are any comments from any of the members of the workgroup or any questions? I know this is going to be a subject of discussion also at the HIT Standards Committee next week, so we can hear more about it. We're having the opportunity to hear some of it today because of the work that we're already doing with digital certificates specifically.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I think at this point, Walter, we've told them all we know at this point.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, let's probably move on, exactly. Okay, well thanks to Arien for those comments. Let's go to the next slide. I'm going to just do a very brief review for those that weren't able to attend our last call, and to sort of recap where we are, so just a couple of slides on the review. At the first call on the digital certificates, we started by reviewing the HIT Policy Committee recommendations on provider authentication and digital certificates, and focused specifically on recommendation number five. Which is the one that asks the Standards Committee to, number one, select and specify standards for entity level digital certificates, including data fields; and number two, certification criteria for EHRs that will test that capability of retrieving, validating, using, and revoking digital certificates, so that's one of the first things we did.

We defined the scope and focus of our workgroup on digital certificates to be primarily on organization to organization exchange and really the class two and class three digital certificates, and still in doing so of course consider all the other HIT Policy Committee recommendations as we develop the recommendations around these digital certificates. We reviewed and discussed some of the key digital certificate related concepts, and there's a long list of those, that talk about PKI, the public and private keys, digital certificates, digital signature, encryption, all these things. We put together and are providing a glossary of terms to make sure that we all are on the same page in terms of the definition of this term. Sometimes things mean different things to different people, and so we wanted to make sure that we had a consistent glossary. It is provided in this particular slide deck as well, just as an attachment to this slide deck.

We also reviewed how PKI and digital certificates work, just to get a good sense of the way those concepts work, the classes of certificates. We noted, and it was sort of an important point made, the temporality of the dimension of the assignment and application of certificates, focusing more on the temporary use of certificates versus more permanent certificate assignment and usage. We reviewed briefly the standards that are available for this, focusing primarily on the IETF, the X.509, and the ISO 17090-123. Those were the initial ones that we certainly identified as being used. We viewed also the core data elements that are involved in the digital certificates, primarily those defined in the X.509 standard. Then we identified some industry initiatives that we wanted to explore, and that's what we're bringing back to this meeting today.

Lastly, we set up as our goal to really achieve the completion of this process and making final recommendations to the HIT Standards Committee by February 15th as a first pass, really more of a status report back to the Standards Committee next week because we won't have really recommendations to represent there of course but just a status report. But then complete the process and present the final recommendations for action at the March 29th meeting of the HIT Standards Committee.

The schedule that we have organized is presented in this slide as well, so we have today's call, which is reviewing on the ground examples of implementation of digital certificates, and then beginning the discussion of these guidelines and evaluation criteria for selection of digital certificates. Then February we'll be presenting the status report, February 16th. February 28th, March 9th, and March 24th are the

three upcoming meetings that we have set up at the S&P Workgroup where we'll be discussing the use case application and the initial set of recommendations in terms of these guidelines and selection evaluation criteria. We'll continue through March 9th and March 24th refining and finalizing these recommendations to submit to the HIT Standards Committee. Then you'll see the March 29th HIT meeting.

Let me stop there and see if there are any questions about any of this background or the process or the next steps.

Ed Larsen – HITSP
I guess I have a question on how we're going to integrate the work of the Standards Committee and this workgroup in that calendar with the S&I framework and its development of use case and guides. How does that relate?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I guess, and Arien, I don't know if you want to jump in and see where there might be some need to realign some of these schedules, if that's the case.

Arien Malec – ONC
Yes, thank you. What I hope we can do relatively quickly is have this workgroup and potentially the Standards Committee as a whole draft essentially a set of evaluation criteria or charter for the S&I framework. I think we all recognize that given the timelines for stage two Meaningful Use and the regulatory timelines that are associated with that. We're going to have a lot of work to do in the next six to nine months prior to what we would assume would be a very similar timeline for a notice of proposal we'll be making for standards and certification and for stage two Meaningful Use. So we need to work in concert and very quickly, I guess would be the summary. But I would hope that one of the actions in this process would be the drafting of this evaluation criteria for the Standards and Interoperability framework and spin up an initiative and execute very quickly against that evaluation criteria.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Walter, I think this slide, and Ed, this slide is best taken as part of Walter's summary of the first call. This slide really has been overcome by events at this point because this workgroup will not be the one making the recommendation ultimately, but rather it's, as Arien just indicated, we'll be providing input into the S&I framework.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
This is making the recommendations of the criteria. This is not the recommendation of the standards, of course, by the—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It still goes to a level I think beyond what the workgroup ultimately will be going in its new role. I think we need to get past next week's meeting and then readjust our charter as well as the calendar. Okay?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So I guess the question, Arien, is still whether if we come back—and this is the purpose of today's call, as you will see later after the presentations—is really to talk about the guidelines and evaluation criteria. Start that discussion, but if we needed to accelerate, and again the intent of this particular timeline is to bring back to the HIT Standards Committee, I should probably have written that, March 29th HIT Standards Committee, not Policy Committee, the recommendations of the guidelines on up front evaluation criteria. Is that, Arien, too late? Do we need to think of ways in which we can sooner than that provide the S&I framework with guidelines and certification criteria?

Arien Malec – ONC

I think we're going to have a lot to do in this upcoming year. I would in general advise for all of these things that you try to expedite to the extent possible, because it's going to take some time to form a community, work through the issues, and come up with recommendations. To the extent that if we find or if this workgroup finds that there's a well-established set of standards and we don't really need to spin up the work then we may not need to go through this process. But if we find that there is a need for this work, it's going to take some time to execute through, and the overall timelines that we have are very tight.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So it sounds to me that by the end of this call we should have a good sense of what are the steps that we need to take in order to finalize fairly quickly these general guidelines and evaluation criteria and the description. I know we have a template for the S&I framework to describe the project scope, I suppose, whereby there's a description of the actual, this is the need. So that's one element that you're looking for, Arien, as I understand, a description of that?

Arien Malec – ONC
That's exactly right.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So we'll have a chance to talk about that at the end of the call then today.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think as we listen to today's discussion we should also try to task the specific technologies that Meaningful Use is calling for. Arien knows quite well that the technologies that one might use for certificates, issuance, distribution, validation, when the use case is SMTP S/MIME e-mail can be very different than the mechanisms one might use where the infrastructure is a Web service infrastructure and you're using TLS as the security mechanism. I think that's also another very important scoping mechanism for what is urgent for us to resolve versus what is not as urgent, so I just want to remind us that the mechanisms used are different depending on the transport technology that you are ultimately securing.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Good point, yes. Again, I think as we really get into the discussion of the guidance and the evaluation criteria, those elements will come into play, this point that you make about the difference in the infrastructure depending on whether we're talking about simple ... S/MIME e-mail versus TLS. I think, again, our charge really will be to define more of that evaluation criteria and that kind of guidance so that the S&I framework can then go and do the whole 10-step process, I guess, or 9-step process of the framework, focusing on the digital certificate concept. Then coming back out with some of the recommended standards that they can bring forth to our committee. We'll keep that in mind certainly in the incorporation of this evaluation criteria and guidelines.

Any other questions or comments before we go to the presentations?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Just to pick up on John Moehrke's comment, I'm unclear, and I think maybe what you're saying is that we'll figure it out this call, but I'm unclear on whether our task is at the level of specifying how certificates themselves work versus how people use certificates in particular use cases. It seems to me that the former is pretty well a solved problem and it's just a matter of finessing some of the details on which fields would be mandatory, etc. The latter is as wide open as every transaction in health care, so somewhere in between those two is our target, and I'm not quite sure what it is.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Keep in mind that the S&I framework includes the S&I framework team developing use cases. So this workgroup's input is to guide that effort, not to develop the use cases. John Moehrke's comment is very

well taken, but I think that our role of this workgroup will be more advisory to that work case development team than in actually scoping the use cases ourselves.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I think John Halamka put it nicely the other day when we were thinking about this, in terms of really in the first round of things. This hopefully will help clarify the transition in our role, in the first round of things last year we really got into somewhat of the nitty-gritty of the standards themselves and discussion of specifications and things like that and recommending those to the coordinator for incorporation into the regulations. I think what's happening with the S&I framework is that now we, as Arien mentioned, we have the infrastructure, the resource that will do all the work in terms of the detail analysis and definition and development of the use case and identification of the standards and harmonization and all this process. Then come back to us with the recommendations. This is what in the past, three or four years ago, AHIP was and what HITSP and the technical committees were doing, the HITSP and the technical committees are now what the S&I framework will be doing with respect to the actual, again, nitty-gritty work, I think. And we will be become much more of a higher level of definition of guidance and criteria and then receiving back the recommended standards after all the ten steps have been completed for final recommendations to the national coordinator. I think that's a shift in this role that we're having. So at the end we might not end up necessarily getting into the details of the standards. On the first call we even started talking about the data content of digital certificates and elements like that that we might not necessarily need to get into ourselves, but the S&I framework will actually get into those details. I hope that's helpful in clarifying this transition in terms of our role.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think that makes sense and it's a welcome input obviously to have a full-time, fully staffed team take on those details. On the other hand, having worked through some of the Direct Connect issues around certificates, an awful lot of the stuff eventually boiled down to just policy decisions. Do we see ourselves making recommendations to the Policy Committee about what they should select as policy, or are we going to try to stay away from that?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
No, I think it's the reverse, David. The Policy Committee makes the policy determinations and they pass those to us for us to define the standards. So now in this new role what we would be defining is the parameters, the criteria by which the S&I framework will look into one of these topics, say provider directories or digital certificates, will define the criteria for the standard evaluation process and then they will go through that. But we receive really the direction from the Policy Committee.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But there's an awful lot of unspecified things in policy that we kept stubbing our toes on in Direct, Arien, I think is going to talk about it later on—

Arien Malec – ONC
Yes, you're giving away all my presentation.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Okay, I'll shut up.

Arien Malec – ONC
Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
We should stick with the schedule. I think –

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
All right. No, this has been very helpful. I know that we have said that we will have a lot more time to discuss this with members of the HIT Standards Committee next week, so let's go to the next slide. I think this is where we will begin to have the presentation. The order I think we have is we'll start with the ONC Direct Project, then we'll go to the VA, and then we'll finish up with the NW-HIN Exchange specs.

Arien, I don't know if you have slides to—

Arien Malec – ONC
Unfortunately, I don't. I apologize for that. But I can verbal through what we did and then also, as David just mentioned, where we have this interesting policy standard interaction. So in the Direct Project the mandate for the Direct Project was to look at and provide specifications for directed exchange between known participants and supportive Meaningful Use. One of the key policy constraints that we had that had come from the Nationwide Health Information Network Workgroup of the HIT Policy Committee was that one of the key dimensions of trust for directed exchange really resolved around identity. That is, that the sending party should be able to have a high level of assurance that the receiving party is indeed the entity or person that the sending party intended to send to, and then that the receiving party likewise should have a high degree of assurance, or at least a known degree of assurance in the sending party. We also wanted to ensure that both the sending and the receiving party had a level of confidence of understanding what happened to the data in transit, that is that nothing nefarious or improper happens to the data in transit that's not under the control of the sending or receiving party.

Very early on we, after a considerable amount of discussion and debate we formed a standard set of principles that we applied to this level of trust dimension. Some of the core elements of that were, number one, settling very early on that the enabling technology would be the X.509 digital certificate. Number two, that the core dimensions really settling on the notion that the core dimensions of trust were to be established as identities and as identity attributes or policy attributes that were associated with the certificate. Number three, establish very early on the notion that we were not going to constrain or define all of the key policies in question. Rather, that what we were going to be able to do was use the hierarchical property of digital certificates and the associated policy with a trust anchor for a digital certificate to establish what we called "circles of trust." That is, communities that had common definitions for identity and the other attributes that are encoded in policy for a digital certificate and enable communities to import trust anchor root certificates that correspond with the policies that were established by the community.

So for example, if my community wants to see a NIST level two level of identity assurance or the appropriate equivalent level of assurance for an organization, then I would choose a certificate policy that corresponded to that level of identity assurance. I would also have an evaluation criteria for other root or trust anchors to incorporate into my technology that I would also trust as adhering to at least the same level of identity policy. So after a considerable amount of debate we established that as the core set of principles. We actually worked through prototypes of different ways of expressing the same security considerations, ranging from TLS, to S/MIME, to various permutations on that with different enabling technologies. Finally settled on, as I think people are very well aware, SMTP with S/MIME and where S/MIME really is the enabling technology that encodes those attributes and gives a nice property that a spender can assure that only the receiver or somebody specifically delegated by the receiver, can actually even see the content unencrypted. That the receiver can verify it through the use of a digital signature that the sender was indeed the one who sent it and that by means of encryption and content level encryption there can be a high level of assurance that nothing untoward happens to the content in flight.

Having established that, at the level of standards and data fields we felt the need in the core enabling specifications, the Applicability Statement for Secure Health Transport, to define the validation criteria for mutual trust. Essentially, what we did is point to the core ITF RFC that defines the operations of X.509

digital certificates in the Internet. We did find the need to specify specific data fields for holding key identity information and the validation criteria against those data fields. So as people know, once you have a digital certificate you don't have to have a high level of trust in how you obtain the digital certificate, as long as you, number one, trust the certificate issuer; and number two, can prove that that certificate issuer issued the certificates of the counterparty that you're trusting. So in the context of an SSL certificate, for example, your browser will examine the DNS name to which the certificate was issued and can prove that the certificate that's been proffered by the server that you're going to corresponds to that DNS name and is issued by a party that you trust. That gives you a high level of assurance that you are indeed connecting to the Web site that you're intending to connect to and that things like credit card information and such are secure in transit.

Having done those activities and institutionalized those decisions in the core specifications, we immediately ran, and are currently running into, an issue that's actually an interesting intersection between policy and standards.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Arien, Can I interrupt you before you shift into that side of the—?

Arien Malec – ONC
Sure.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
On your nice summary of our years' worth of meandering on the Direct team, I think it's a fair statement to say that basically what happened during that year was massive education on how this stuff works and that when it's all said and done we're using standard X.509 cryptographic techniques right out of the standard libraries. It was just a question of getting everybody on the same page to understand how that worked and what the terminologies meant and agreeing a little bit on a way to quickly flesh out an infrastructure with reference and ... that made all of it a don't care for the average person who wanted to use it. But we didn't invent anything, right?

Arien Malec – ONC
That's exactly right. As you said, we educated ourselves very heavily. Some of us, like Mike Davis came in pre-educated and John Moehrke came in pre-educated, and the rest of us had to get a quick education.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It took a long time to do that because stuff is tricky and the language is confusing and some of the phrases have multiple meanings depending upon the context. I think that was the real struggle was it took a long time for anybody to understand the stuff. But we didn't do anything that's not really off the shelf use of X.509, as far as I know.

Arien Malec – ONC
That's exactly right. What we did was essentially follow the core specifications and essentially specify that implementations follow the core specifications for X.509 certificates on the Internet, including the specified data field that mapped to identity, and we did those in an incredibly standard way.

So I'm now going to make the shift into this interesting policy technology area. One of the things that we then are being asked by is organizations who because of the way we designed this, and again designed this following standards, to ensure the broadest degree of interoperability we have organizations who are now asking the really important question, okay, thanks for all of this but which anchor should I trust. As I think people understand in the Web area all of our browsers come pre-configured with a set of trusted root certificates, that our browser makers, the Microsofts and Mozillas and Googles and such of the world, have decided adhere to strong policies for issuance of certificates. The parties to exchange both at a state policy level as well as at a HIST level or an organizational level are now essentially asking that

same question, which is, okay, so now what? How do I choose the master list of trust anchors that corresponds to policies that I care about?

Coupled with this, and I'm sure Mike will have more to say about this, the federal government, through the Federal Bridge Certification Authority, has established a uniform set of standards for issuance of certificates for federal partners. I'll abstract away the details and say that what the federal government has done is provide an infrastructure for cross-signing of root certificates, which means that one certification authority can cross-sign another certification authority as being a trusted member of the Federal Bridge Certification Authority. Then number two, a mechanism for encoding a whole set of policies in what are called policy-oids that are carried in the digital certificate.

So I'm going to back up a little bit. There are two documents that are associated with certificate issuance policies. There's a certification practice statement, which describes the practices of a certification authority, that is Verizon, or VeriSign, or Go Daddy, or what have you, in trust of the world who's actually doing the certificate issuance. Then there's a certificate policy statement that describes the policies under which a particular class or chain of certificates is issued. Part of what we discovered through learning is that there are good standards certification practice statements. There is the WebTrust standard, and then a highly associated ..., European standard for certification practice statements. Those things cover notions like how does a certification handle its keys to ensure trust, what processes do they use to sign the digital certificates, how do they enforce certificate policies, those kinds of things.

But a given certificate issuer can issue certificates using multiple policies, and in the Federal Bridge architecture a given root may actually issue certificates with different policies. What the Federal Bridge has done is noted policies that map effectively to NIST levels of identity assurance. So there's a rudimentary that maps more or less to one basic, which maps more or less to two medium, which maps more or less to three, and a strong I think, or whatever it is, that maps more or less to NIST level four ... sub-flavors for machines and for HIB cards and the like. But that's essentially the gist of it.

We recognize that broad interoperability with federal partners is going to require interoperability with the Federal Bridge Certification Authority. We also recognize that the Policy Committee has handed down I think very appropriate recommendations related to policy for certificate issuance for organizations. And we've been looking at norms for certificate policies, for certificate issuance in the organizational level and we've identified at least two decent models; number one being the Federal Bridge; and number two being what are called "extended verification" or "extended validation" certificates that are issued for the purposes of SSL validation. That policy gives very good enabling policies for issuance to organizations. Where we are right now in the Direct Project is identifying a need to either have a browser like bundle of pre-trusted certificates, or establishing something similar to the Federal Bridge Certification Authority or using the Federal Bridge Certification Authority. Which is to establish a common set of policies and an enabling means for identifying which policy was used in a particular certificate to enable the broadest degree of interoperability.

So we've moved from specifying the base level standards that can be used in a bunch of different ways to very quickly having organizations going, okay, but we really do want to carry this out to a wide degree of people across the United States. So we really do need to start looking at what that browser bundle or what that HST bundle might look like. So we've moved very quickly from just staying at the standard level, this interesting intersection between standards and policies, and that's where we are right now. With that, I will conclude.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thanks, Arien. Let's see, are there any questions from anyone?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Arien, your last statement about this browser bundle or the sets of policy statements, are you moving away then from the DNS provisioning certificates model?

Arien Malec – ONC
This is a somewhat orthogonal issue. The browser bundle, if you will, the concept of a browser bundle is a concept of free trusted roots that are known to correspond to a particular set of policies. It doesn't get away from the need to when I send I need to identify that certificate associated with my receiver so that I can encrypt the transaction. I couldn't get away from that issue.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
It just means the roots that are trusted.

Arien Malec – ONC
That's right.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Okay.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I'll jump in on that because that was the question I was getting back to at the beginning, which is the part of this that seems to be a solved problem is how do certificates work and how do they encode and represent various levels of assurance and so forth. The policy question seemed fairly clear, the answers aren't necessarily clear, but the questions are pretty clear. The thing that we did in Direct I think was to work out a specific best practice use case on how to actually take advantage of what's embedded in those certificates. My fear is that there may be hundreds of those use cases over the course of the next couple of years of HIT software development, even though they're all relying on the same core capabilities of certificates. So do we feel the need to take on things like figuring out how to distribute certificates in a cost efficient way for direct e-mail, or is that really somebody else's problem. That was the... where is our scope, is it the detailed use case level, which is really best practice around a well understood technology, or are we actually questioning the core technology.

Arien Malec – ONC
By the way, not to make this more complicated but I'd also note that the Department of Commerce, through the Cyber Security Initiative and NSTC, is also looking at many of the same issues relating to uniform guidance, or at least consensus guidance, on trusted identity for electronic commerce and other kinds of cyber space uses. So this problem that we're facing in healthcare is a very important part of a wider and larger problem for commerce and Internet transactions generally.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'll ask this to both David and Arien, so within this emerging framework of the interaction between the Standards Committee and the S&I framework, would you see the Standards Committee recommending the scope that David refers to? At what point do you stop with the standard that comes out of it in the S&I framework?

Arien Malec – ONC
I would think so, because frankly this notion of what's a universal browser bundle is a heavily policy oriented discussion and it's one that I don't think the S&I framework is equipped to handle. But it certainly is equipped to say here are the standards that are associated with this, and here are some best practices that at least have been identified in the broader community. As David McCallie notes, I think the standards and the art for this in terms of where do you put a domain name, where do you put an e-mail address, those kinds of things and then how do you validate them are reasonably well described in standards where I think the need may be to specify, to John Moehrke's as general a way as possible, what a good certificate usage in healthcare might look like. But I also would note from the Direct process learnings that once you identify the standards you really, really quickly shift to policy, and policy becomes the urgent need.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Unfortunately, this level of policy is foreign to the level of policy that comes out of the Policy Committee.

Arien Malec – ONC
Yes, that's the problem. It's a really strange interaction between technology and policy.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, it's really technology policy, not operational policy really.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I would very much agree with what Arien said and add just one additional thing. I think this committee can identify—when you get into managing certificates, discovering certificates, you do get into the space of there are a few technologies that are available. It may be very important for us to remind the S&I framework that yes, they do need to support one or two or three of those because the policy decisions are not cut-and-dried.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, I agree with you.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So it's not a matter of just simply saying don't do anything because policy is up in that space. We can say well, here are three ways that certificates are likely to be managed and are commonly managed today. Yes, you have to support all three. I think that's also another lesson we learned in Direct, correct, Arien?

Arien Malec – ONC
Yes. The lesson I learned was that most of those decisions had already been thought through by smart people ten years ago and I just didn't know about it. So we had to rediscover the fact that there are standard levels of assurance and there are standard approaches to categorizing the different degrees of security, well, assurance is the best word, that could be selected to apply. I think for a lot of the process of Direct it was just learning what's already out there and figuring out how to map it to our use case.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right, and having this committee say, yes, you will learn these lessons, here's the results, go ahead and learn them if you need to.

M
Yes.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm hearing at least two more. In addition to maybe looking at this set of guidance and evaluation criteria that we've been talking about, there are a couple of other levels of recommendations that we're thinking of providing that will be valuable, this concept of universal browser ..., some recommendations around that. Then recommendations about the types of, more a reminder of noting of the fact that this might be a guideline of the fact that there are one, two or three different types of technologies that the standards will need to support, so it's sort of identifying those types of technologies to make sure that they are considering the evaluation process of the standards. Those are two additional types of recommendations.

Arien Malec – ONC
I think so, and I think Mike's going to help educate you on the Federal Bridge Certification Authority. I think one of the things that this committee might want to look at, and the S&I framework might want to look at, are what are the industry models that have been successful at establishing high trust certificate. Because as we know in the browser world we got down to a level where certificates were issued based on the mere proof that you had control over a domain and the browser makers and certification authorities

felt the need to invent this extended verification. So what are the best practices, I guess, for establishing high trust certificates and what kinds of, in this strange technology policy area, what kinds of certificate issuance policies are associated with those best practices, I think might be another area for recommendation.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The other lesson that we can learn from, or the other worked example that we can learn from, I think Dixie sent out the federal register or transcripts around the DEA decision making process for their very concrete and very precise recommendations on levels of assurance for ePrescribing of controlled substances. That was a politically heated, controversial, multi-year, contentious process, but it finally resulted in a very concrete set of recommendations which everyone is now busily implementing and I think reasonably happy about because all of the vagueness was taken out by the recommendations. But it was a complicated, expensive, nasty process. I don't know how you can skip past that. But at some point, you just have to say this is what we'll all do. And the question I have is who makes that decision? It's not us. I don't think it's the Policy Committee. But maybe we, with the Policy Committee, have some recommendations on what makes sense for HHS, CMS, ONC, and whoever's the right landing point to give –

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
A problem with assurance is that the high level policy like the Policy Committee makes is, yes, we want to be very, very sure that that is who we think they are. It's very high level. But when you really build in assurance into a high assurance system, it touches everything. It's the components you select. It's the integration that you do. It's the methods that you use in development. Yet, those are policy decisions but they're not at the high level, they're really at the implementation level policy decisions that you make in order to get an assurance level that the policy says you need. So I think there are two levels of policy and I think one level of policy is probably within the realm of the Standards Committee not the Policy Committee.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
The Policy Committee also made recommendations on a number of other areas that are certainly very linked to this. One was, for example, on recommendation number four, establishing an accreditation program for reviewing and authorizing certificate issuers. There are a number of other kinds of policy recommendations from the Policy Committee not coming directly to the Standards Committee but going directly to ONC that will be put into the mix of the various activities. I'm sure this is the kind of thing that the S&I framework will be looking at as well. So there are some other policy level recommendations that have gone directly ... ONC to look at how to implement them, and they might complement this type of policy technical level of recommendations we make.

Anyway, are there any other questions for Arien about this? Any other comments?

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Just one last thing is that when we get to individual level certificates it gets even more complicated, in terms of the policy side. The technical side is not complicated, or it's solved. It's complicated, but it's worked out.

M
I guess I'd like to stress what Dixie was saying, that there is a spiraling between this high level policy of, yes, we need these to be absolutely as high as possible with the pushback from technology that says, well, if we do that this is the technology result, the expense, the overhead, is that result equal to what you are protecting go back to policy. So you kind of end up doing a risk reward tradeoff to get to ultimately what is the stated policy of yes, actually this is really what we mean. I think we need to be ready to do those iterations between standards and policy to help create the ultimate policy that we'd really speak about.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
A question, John, and this may be also for Arien is to what extent that happens in the HIT Standards Committee environment and the workgroup environment or whether that's part of really what the S&I framework is going to be doing. And one of the criteria would be cost and feasibility of technology implementation.

Arien Malec – ONC
This is why I mentioned the Cyber Security Initiative and NSTC. This notion of a strong, robust market for high assurance identity, the market dimension of this can't be overlooked. We would need to craft both technology and policy that helps create a strong and robust market for high assurance identity and in ways that make it more highly available to a broader degree of participants than it currently is right now.

Joy Pritts – ONC – Chief Privacy Officer
I believe that Howard Schmidt, the Cyber Security czar, spoke on this issue earlier in the week and clearly indicated a preference for market based solutions.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I think what to me was so enlightening and pleasantly surprising when I read the Federal Bridge documents as well as the NIST documents, was how flexible they were in basically saying here's an aggregate set of choices that you can choose from within that we all deem to be of medium level, roughly equivalent assurance. That's a really smart way to do it, because it does the hard work that a scientist needs to do and lets the individual implementer have a range of choices. I fear that we're not even at the level of saying you need to be at least medium or you need to be high or you need to be basic. We don't need to tell people what kind of token to give, but we do need somebody, the "we," the royal plural, somebody along the way needs to say this is good enough, medium level assurance for direct push communications or maybe that we would require that it be higher than that. So the NIST approach and the Federal Bridge approach seems really to have grappled with that question of the interaction between different technologies and their associated cost and burdensomeness with the policy goal of having adequate security, adequate assurance. We should follow those examples where we can, I think.

Arien Malec – ONC
I do apologize. CDC scheduled a meeting over this meeting at late notice, so I need to drop and attend that one, but this has been a great discussion. Thank you for inviting me.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thank you, Arien, for joining us and for providing this background and this perspective on how this is happening in Direct. This is the perfect setting, I think, for our next presentation. So I'd like to invite and also welcome Mike Davis as a new member of the workgroup and invite him to provide us with the VA perspective on digital certificates and probably answer some more questions about how the Federal Bridge is working and is tied to this. Mike?

Mike Davis – VA
Thanks, Walter. It's a pleasure for me to attend my first meeting of the workgroup as a member, and kind of throwing me in the ocean here to give a presentation at the same time.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
We always put our new members in that position.

Mike Davis – VA
That's what I figured.

M
If we don't like your presentation, we're going to kick you out.

Mike Davis – VA

Yes, that was a concern because sometimes the dew points a group gets to and an understanding of vocabulary may not necessarily be known to those that aren't closely associated with it. I did work with the Direct Project Security and Trust Working Group and Arien since its inception. And there have been several references to the National Strategy for Trusted Identities in Cyberspace, and I would just say that I was also a participant in that for over a year now. Those things are very relevant, I think, to the discussion that we're having. I present myself as a VHA security architect. I am on the business side of the house in the healthcare system, and that's what we've asked to see here. I don't speak for the projects that I'm going to be discussing a little bit, the healthcare ..., and so bear with me on that, nor do I speak for the Federal Bridge or any of those groups. At the VA level, we are trying to implement those things.

To reiterate that, the VA is a federal agency, a department of the federal government, and we must comply with numerous federal regulations, laws, etc., some of which are identified here, NIST, special publications, fixed publications, OMB memorandums, laws, such as HIPAA and HITECH, etc., all those things have to be bundled together into the VA system. Unfortunately, we have no shortage of those kinds of things, so we're good to go there.

The Federal Bridge has been mentioned a couple of times, the Federal Bridge and the Federal Identity and Credentialing Management Program, ICAM, and Federal or ICAM does provide federal agencies with a consistent approach for managing and vetting credentials of individuals. I've given you a link there to that, and you can find out more about HSPD-12 and ICAM. But the VA, as a federal entity, again falls under ICAM. I would also mention that the national strategy, the NSTC specifically references ICAM as well as ... and federal entities participate with respect to that. So with respect to things like the Direct Program, for example, there are some implications for the VA with respect to the trustworthiness of credentials that we would use and of course, those are trustworthy credentials through the Federal Bridge. I would mention that just for interest that at the upcoming HIMSS conference, the ONC sponsorship, the VA is presenting a demonstration of NHIN Direct and they're using ICAM compliant credentials.

The VA has to integrate all this into our infrastructure and correlate it so that the VA has our view or our adoption of ICAM. We correlate that to our identity in access management internally and so there are correlations between ICAM and what VA is doing internally there. They're fairly one to one, with credential management, identity management, federation activities, access management, auditing and reporting, and the services that we get out of it, such as single sign-on, we've broken that into internal single sign-on, meaning people who we issue credentials to and external, which would be external people who are not directly known to the VA. Our models internally reflect the federal laws and direction that we comply with.

So getting into specifics about the VA and digital certificates, first of all, who do digital certificates apply to, and in the VA it's practically everyone, including veterans, employees, contractors, affiliates, and you get your credentials, certificates for an identity proofing process. We follow obviously the ... standards for this for different levels of assurance, and as a result you get different types of credentials and the information about your credentials is then provisioned to back end systems. If you are an employee or a contractor or affiliate, then you would get an HSPD-12 PIV card. If you are a veteran we don't issue certificates directly to them, but veterans also have PKI credentials, and I'll speak to that in another slide in a minute.

M

Just a question, and it may be out of place, but it sounded like you have different degrees of identity proofing depending upon the person who needs the proofing. If so, is the degree of assurance encoded in the certificate that they get using the policy-oids that Arien was talking about, or do you do it some other way?

Mike Davis – VA
This primarily comes into play with the difference between employees and veterans themselves. So for employees they're all issued level four PKI credentials under HSPD-12, and that's it, so they're all at level four. For veterans that's a little more nuanced depending on the type of information they need to get to and what they're doing.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Mike, a quick note also on the employee side, doctors and healthcare providers, are they using that same level of level four security?

Mike Davis – VA
Yes, there's only one level in the VA. The federal government, we have to comply with HSPD-12, Homeland Security Presidential Directive and NIST PIV 201-1, so all persons known to the VA get that credential. We do not have a healthcare specific PKI system or anything like that. Now, a number of years ago I participated in some standards committees' work which attempted to profile standards certificates with healthcare specific, non-critical extensions, so maybe put in credentialing information. But as things have worked out, the federal government is issuing a single credential, and you can theoretically get that credential at any federal agency, they are all the same, so that these non-critical extensions that might belong to healthcare right now are being carried over into directory services rather than extensions of the cards or the credentials. Does that make sense?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, that makes sense. When you say "non-critical extensions" are there critical extensions then?

Mike Davis – VA
Sure. The core standard defines critical extensions and then you can have non-critical as your optional. We found when we did this, though, that if we wanted to add non-critical extensions to the credentials, that we actually needed to go to the credential provider to enable those things. So that means if healthcare were to establish non-critical extensions then the providers of those certificates may have to specifically support that.

M
Do you provide your own certificates or do you use a commercial provider, the VA, that is?

Mike Davis – VA
I'll get into that. Good question, but I have a slide about that.

M
Great.

Mike Davis – VA
Maybe we can go to the next slide. Of course, certificates are used for a number of business applications not relative to healthcare. I've thrown in e-mail as one of those, although you can make an argument that it's used that way. But there are financial and other uses, so primarily with respect to employees, contractors, and affiliates we speak directly to the issuance of the credentials and the personal identity verification program, which the VA calls PIV. Then implications with respect to projects and programs such as the Nationwide Health Information Network, both exchange and direct, and our umbrella program, which is the virtual lifetime electronic record, electronic prescribing, which I'll talk about briefly, which somebody brought up already, and then a joint VA, DoD activity that we have ongoing. Then with respect to veterans, the single use of credentials is for electronic signature and we're not issuing veterans PKI credentials or anything like that. That would not be something that the VA would do. These are the healthcare relevant activities I'll focus on within the VA health system.

The first one is the PIV program that I mentioned. This is a department-wide initiative to integrate Homeland Security Presidential Directive HSPD-12, and incorporate that within the VA's enterprise architecture. As to components, first is the issuance and provisioning of the cards themselves, the mechanical process of identity proofing and activating cards and capturing data and stuff. Then secondly, to provide an identity and access management infrastructure to deliver identification and authentication, access control authorization, and audit and enterprise services. The card has to be enabled then with services to make it meaningful in a security infrastructure otherwise, it's just a card. So we have these two components, so the notion of enterprise services that support these certificates and credentials that are used to support security services.

To the question asked, currently we're using Gemalto and Oberthur brand cards, both are 64K. We're going to be going over to Oberthur cards version 5.5 in March. We currently have 204 ... offices throughout the country, including Alaska and Hawaii. We've issued approximately 175 cards to date, with a target goal of nearly half a million. All of the federal agencies' status is available on the link that I gave you a couple of slides back. You can find all of the federal agencies completion dates. OMB is set for the federal government, with a completion date of September 1, 2011, by which time all federal agencies are to be 100% deployed. As you can see by this number here, we're about 40% there.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Are you talking about just VA, or are you talking about the whole U.S. federal—?

Mike Davis – VA
No, this is VA.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
VA only, okay.

Mike Davis – VA
Right, but the entire status of the deployment is available on that link I gave on the ICAM slide, www.idmanagement.gov. You can go there and you can see the VA as well as everybody else, all the other federal agencies. Okay, so we have as the first step we have to issue the cards and the certificates.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I assume you also issue them to software servers, right?

Mike Davis – VA
Yes.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
The cards are just for individual probably signing certificates, right?

Mike Davis – VA
These are the certificates that a person would use, yes, for signing, for identity, for encryption.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Do you use basically the same process to issue certificates to servers?

Mike Davis – VA
Basically, yes, that's right. This slide, I wanted to speak a little bit to the use of certificates and credentials in the NHIN. First of all, VA clinicians participating in the NHIN obviously use their credentials to gain access to the system, so that's the obvious place there. They're using the PIV credentials, and that's it, that's what they're using. Then we receive requests from the NHIN from folks through the gateway system and those are SAML identity and attribute assertions, which include credential and

certificate information, of course, and then it's parsed into attributes to make access control decisions with, so I've indicated some of that stuff on the right. In terms of enforcement, this is where the VA is planning on implementing patient consent directives in accordance with HIPAA, a full set of possibilities for authorizations or revocations or restriction requests through an electronic system with an electronic signature on those types of consent documents. So those go through a process—and I'm just showing how the ... and the credentials play together to inform and provision the access control decision information and an authorization system. And how the credentials are used to gain access to the system and at least prove that you are someone that has the minimum right to even talk to back end communication systems. So at the service level this gives us the ability to control access to individuals, turn on, turn off, or suspend access at the national level without dealing with tens of thousands of back end applications.

This is highlighting, again, the veteran's role in here. The veteran submits their consent directives through some portal accessing a form service. Some of the forms are the ones I mentioned there, healthcare specifics such as authorizations, restriction requests and revocations. We currently use a policy of opt-in for the NHIN, so through these services we've established that veterans can use a VA managed PKI. So with the software PKI, VA managed on VA servers and we provide and manage credentials on behalf of the user, so it's like that. The veterans log in with credentials that they've established initially probably through the DoD, so all of our customers, well, most of our customers are former DoD service members who have been issued ... cards, HSPD-12 compliant cards, and gone through a proofing process.

While they're in the service they also get DS log-on credentials, which they use the same proofing process and get those credentials. The VA is now using DS log-on credentials when they come to the VA, that has become part of our system, and actually the portals themselves authenticate when a veteran who is now a veteran in the VA authenticates to the VA portals they're actually authenticating using their DS log-on credentials back to the DoD. So we are integrating these credentials together. The VA manages a signature service where, like I mentioned, veterans are provided with PKI credentials. At the time of the signature they re-authenticate using their DS log-on credentials, and then the signature is applied by this appliance with their electronic digital signature, and then the user's consent directive is then passed on to the release of information office and then it's provisioned into the access control decision for a system for the NHIN.

We have different levels here, so our legal office, the Office of the General Counsel, has approved the proposal on our part to say that we would only use the electronic and the digital signatures for those documents whose risk value was such that we felt it would require such. So for simple opt-ins we're using currently more an "x" in the box, not the digital approach, an "x" in the box like an end user license agreement, and we're in the process of standing up these services. Of course the signature service applies to other forms that a veteran may sign besides just healthcare ones, but once the system is up and fully operational we will probably migrate to using the digital signature service for everything, so that's it.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
The vets all have a hardware token in the form of a card, is that their—

Mike Davis – VA
No. Let me be very clear about that, the veterans do not get a card. Their certificates, these certificates would be level three, they're managed by the VA in an appliance, which provides a software PKI credential. So they do not carry or hold anything of their own. In accordance with the NIST specifications here they use a level two or a level three authentication process to request the digital signature which is provided by the appliance on their behalf, so they do not have a card, they're not issued directly anything that they would carry on their person like that.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

What is this appliance? I'm not sure what you mean by appliance. Is that a physical device by their computer or something where virtual—

Mike Davis – VA
It's a physical device managed by the VA on the VA network. The VA manages this on behalf of the veteran. There are numerous products out there and I think standards for this kind of thing. If you look at OASIS Digital Signature standards it talks about this kind of thing, so that's what we're doing. What it gives us is greater assurance that the veteran is in fact the person signing the document and also provides greater strength that these documents aren't modified. Now, again, it's a risk management decision as to whether this technology is sufficient for the purpose intended. So for the consent directives in healthcare we believe it is. Maybe if you were talking about a power of attorney or something like that, maybe not. I don't know. We haven't analyzed those types of documents.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I see the note on the slide that it's coming to the My Healthy Vet application in the future. How will that work if that veteran comes in through a Web interface? Will they just authenticate with—

Mike Davis – VA
Currently the veteran authenticates to My Healthy Vet with a My Healthy Vet password. They can also get in through the federal ... program. But where we're going, the eBenefits portal right now totally uses the DoD's DS log-on to authenticate, and so we are converting My Healthy Vet to do the same thing. So the veterans will authenticate to VA systems using the DoD DS log-on credentials.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Mike, is that DS log-on a SAML implementation or something else?

Mike Davis – VA
It can be.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Oh, okay. I was just wondering what it was. This is at the user interface level, which I think is abstracted away from our task. We're trying to figure out how to authenticate in an infrastructure, so we shouldn't focus too much on the user experience.

Mike Davis – VA
Right. I'm not focusing on the authentication piece so much here, as I am on the signature service ... using digital credentials. That's where the digital credentials are being used for the veterans, it's on the signature service not on the authentication side.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Do you have more slides, Mike?

Mike Davis – VA
I have a couple more.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, go ahead. I'm sorry.

Mike Davis – VA
Let me go on and I'll try to speed up here. We mentioned the electronic prescribing of controlled substances, so the VA did work with the DoD in a pilot that started in 2002 which assisted the DoD in the development of their regulations. Our projected use, and these are older numbers but they shouldn't have changed too much, we have about 41,000 providers that would take advantage of this and at the time we were issuing about two and a half million schedule 2 controlled substance outpatient

prescriptions. The pilot was in a single location at Hines, a Chicago hospital, and in general schedule 2 substances are about 20% of all the prescriptions that we provide. The electronic prescribing is highly valued by clinicians, not so much as improving their workflow but by making electronic prescribing and electronic workflow, and patients get their medications faster this way. Previously there would be delays of up to maybe three days.

Well, the DEA IFR is out. It's now in effect. What the DEA did, though, was to make the requirements for credentials apply to all schedules, not just schedule 2. The DEA is choosing our PIV cards to meet those requirements here. So we have two factor authentication, which is the ... and the PIV card, the requirements call for the separation of hard token from the computer when things are going on and ... compliance, which the PIV card easily meets, and digitally signing of the credential, the PIV card is doing visual signing. In short, the PIV card has been integrated by the VA into the system, where we're currently in the process of making the modifications to the back end healthcare systems, issuing the credentials and rolling this out, but we're able to meet these electronic prescribing requirements entirely with respect to credentials now with the PIV card.

Finally, just a note, we do have joint activities with the DoD. In North Chicago, for example, we do have a joint facility where clinicians access both VA and DoD EHR systems. They can authenticate using either the VA PIV card or the DoD ... credentials. We provide a single sign-on to a number of applications using a CCOW standards based infrastructure and just in that regard with respect to credentials, and John Murphy participated in this, we just recently completed within HL7 a new standard that integrates SAML assertions into CCOW, which was approved by ... in January of this year. This allowed us greater flexibility within CCOW using credentials from backing applications there in healthcare, so the VA and the DoD in this case are using CCOW to facilitate clinical workflow.

That's all the slides I have. Thank you.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Do you know anybody else that is doing that integration of SAML with CCOW?

Mike Davis – VA
Well, I don't. It was very successful at the joint facility. The VA had already started to do this internally as one of our projects, and at the joint center when the DoD became aware of it they evaluated what we were doing and they felt that it would make sense for the DoD there as well. At the joint center it allows clinicians to establish context for patient open applications in the patient context without having to log in and sign in. In our own experience in the VA we found that this is very helpful to the clinician workflow and can save up to 40 minutes a day of clinical time, which is very valuable to us. In HL7 we established this project to formally enable the SAML assertions and the CCOW standard to allow greater flexibility and incorporation into service type architectures. The standard, like I mentioned, just had been passed, but it hasn't been implemented in products yet. It's too quick.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
It's too quick, okay. I'm thinking this is a great thing to see happen. So it hasn't yet been incorporated into products.

M
I don't think that CCOW is really a relevant standard to cross organizational exchanges. CCOW is the standard use for enabling a workflow on a single workstation amongst multiple applications. So obviously I was involved so I think it's great, but the relevance to this workgroup is very thin.

Mike Davis – VA
It may be thin, but I brought it up because we have two different organizations on the joint side that are now using CCOW together and different credentials to integrate a common workflow.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
This is Dixie. I think, as John Moehrke pointed out a while ago, this presentation really is focused on individual authentication, digital signatures, and with the CCOW individual use of multiple programs and having them communicate. But there are certain pieces of it that are most certainly applicable to what we're trying to do between organizations, so thank you, Mike, I appreciate it.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Are there any other questions for Mike? I do have actually one question on the VA and NW-HIN. This is pretty much the approach, the one that you explained a couple of slides ago, is the one that is being used in the VA KP project, right, Mike? I just wanted to make sure, because that is an inter-organizational exchange between the VA and Kaiser Permanente in San Diego.

Mike Davis – VA
Right. There are a number of rollouts of these pilots that are planned and ongoing, San Diego, we've also done one in Virginia area as well, and others are planned going forward, so it is that. Some of these things are VA specific because we are under certain restrictions and laws from Congress under Title 38, that applies specifically to the VA with respect to how healthcare information is exchanged. But yes, Walter, the NW-HIN projects are similar to the one that we have in San Diego and they are maturing as we go forward, so all of the features that I've been speaking about are not totally available yet. They're expected in future iterations.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
So when you exchange data outside of the VA, what applicability, or how do you implement, or are you implementing any digital certificate with other entities outside? Is that something that you can think of?

Mike Davis – VA
Only in the sense of the trust framework that's involved there. So with NHIN Direct and our pilot of that that we're demonstrating at HIMSS, we're using credentials that would be acceptable under the Federal Bridge, so that's a restriction on the credentials. We're not issuing credentials ourselves to other parties. They would get their own credentials as long as they were compliant with the ICAM and Federal Bridge requirements, they would be acceptable.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
That seems to be an important condition, if you will, or criteria, is the acceptability within the Federal Bridge. It's something that has already been mentioned as one of the characteristics or conditions to consider in defining these types of standards.

Mike Davis – VA
Yes, so we're continuing to exam this but I can say at this point that we know we're not wrong if the credentials comply with the Federal Bridge.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I want to ask a question just more generally, and it's a question of what advice or what thoughts about what you would do if you have two secure worlds that intersect but don't share the same level of assurance. So you're a level four inside the VA, and I suspect it's unlikely that that would be the level of assurance that would work in the broader community of healthcare. I may be wrong, but let's just assume for the sake of the question that level three is the level of assurance, how do you create connections between the two worlds if they don't share a common assurance level? Is that impossible? Is it doable through gateway like mechanisms? What's the right way to think about that?

Mike Davis – VA
At this point, I can't give you a good answer. It's a good question. My answer is that right now federal agencies must comply with regulations that we have upon us. That means the Federal Bridge, so a

partner who right now would come in and is not able to present a trustworthy credential to us, it does not appear that we would be able to accept that and be in compliance with Federal Bridge policy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
I completely don't understand the Federal Bridge in sufficient detail to even ask this question but I'll try anyway. It's my understanding from Arien's presentation that the Federal Bridge policy-oids could reflect different levels of assurance. So you could be a level three under Federal Bridge or you could be a level four under Federal Bridge, and my question was assuming that there's a mismatch of the level of assurance, even if you're a Federal Bridge, what do you do there? I understand the legal requirement for Federal Bridge, it's really important to understand that, but I was trying to get one level deeper. And I may not be forming the question right. If so, help me form it right.

Mike Davis – VA
The VA and federal agencies can comply with whatever the policies of the Federal Bridge are. So if the Federal Bridge allows for the use of level three credentials and that is sufficient to provide assurance for the information, the fact that the VA has a level four credential doesn't matter, right, it still works, so it's strictly having to do with the policies of the Bridge itself. Federal agencies under HSPD-12, as far as I know, are all level four, but that doesn't mean that we can't use a level four in a level three environment. If someone has a level three, and I don't know this, okay, but if someone has a level three credential that's authorized on a Federal Bridge, then it would be ... and that was acceptable in the healthcare environment in terms of the exchange of health information, then that would be fine.

John Moehrke – Interoperability & Security, GE – Principal Engineer
I think said another way, we need to keep in mind that we need to separate authentication and identity from the authorizations that it might enable. The Federal Bridge is there to say these are authorized identity issuers and therefore if you can trace a credential to one of the Federal Bridges it is an authentic ID. You then use the attributes contained within the certificate with what is being requested with the intended use of the request with the context of the request, i.e. it's being made from an iPhone on the golf course, versus being made from a secured location inside of a military base. So the authorization decision is a step after proof of identity.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
And you're suggesting, John, that the authorization could take into account the policy-oid level of assurance in—

John Moehrke – Interoperability & Security, GE – Principal Engineer
Exactly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, that makes sense. For some of these like Direct, where it shows up in the inbox not mediated by human decision, well, I guess an algorithm can do that, but net-net there could be—all right, well never mind. It comes back to policy—

M
Yes, the same authorization decision does need to be made in the case of Direct. We haven't discussed it much in committee simply because we've got so many more important things to do, but effectively we somewhat discussed that well, if the directed e-mail was pushed to a medical records clerk, that medical records clerk can be making decisions. Remember, we have those policies that said well, this organization could choose to reject it because the content isn't right. Well, one of the other reasons they could reject it is they could say, well, yes, this is a perfectly legitimate entity this is coming from, but it's the janitor at that facility and I'm not going to receive medical records from the janitor at the facility, even though it' s a highly credentialed janitor. So even in Direct we have to separate the identity validation from the authorizations that that identity enables.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But if I may push on that one a little bit, you used the phrase "authentic ID" but it's authentic at the sense that Federal Bridge policies had been followed by the issuer, the CPS, and the level of assurance of the actual individual ... can vary dramatically even within the Federal Bridge. It can be all the way from basic up to the seventh level, which is whatever that is, multiple forms of ID in person, blah, blah, blah. It seems like that you have confidence that the rules were followed, but that doesn't mean that the person holding the credential has necessarily been thoroughly vetted. They've just been consistently vetted by whatever policy is attached.

Mike Davis – VA
I don't know about that. The identity proofing process means that the individual has been identified at a level of assurance according to the identity proofing and he's got a credential that supports that. So you don't get a level four credential without serious in person proofing and all of that kind of thing. The fact that you possess that credential is proof that you have gone through that process.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
David, it sounds like you're trying to separate the identity proofing from the level of assurance.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
No, no, I was trying to say that within the Federal Bridge. The way I read the document, and I may have misread it, I'd be the first to admit that, that it is possible to have different levels of assurance, different levels of identity proofing, all the way from basic up to whatever their top level is, seven, I think.

M
... PKI credentials at level one, and right now ICAM addresses issuing of credentials up to level three non-PKI and level four is PKI.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So you're saying there is no PKI less than level four?

M
Correct.

Mike Davis – VA
There is PKI at level three. It's possible to have that. That's PKI used, as I mentioned, for the veterans at a level three but it's not on a hard card or a hard token. When you start issuing hard, cryptographic tokens you are at level four.

M
Right.

John Moehrke – Interoperability & Security, GE – Principal Engineer
David, I think at the theoretical you can have a single policy that allows for issuing of multiple levels of assurance credentials and in the credential is the identity of which assurance level was issued.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Correct.

John Moehrke – Interoperability & Security, GE – Principal Engineer
That you will get the notification of whether this is issued under the policy and at what level under that policy.

David McCallie – Cerner Corporation – Vice President of Medical Informatics

Right, that was my understanding. So that could allow, theoretically, someone with a certificate issued under the Federal Bridge rules by a registered certificate authority to present with level three assurance to a system that otherwise operates at level four. You could, as John points out, make an authorization decision to reject that.

John Moehrke – Interoperability & Security, GE – Principal Engineer
Correct.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
So in the policy world that we'll be facing in Meaningful Use stage two when we're requiring people to do exchange, we're going to have to decide whether it's level three or level four.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Or a minimum, you can set a threshold too.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, absolutely, everything is a threshold. And when I say "we" of course you know what I mean, I mean somebody.

M
Yes, and that's why I suggest that we need to separate the identity from the authorization that it is enabling, and too often the CA trust training is dual purpose for do I trust that these identities are authentic and is it authorized? It's because that dual purpose is sometime mistakenly done that things get out of hand.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and I understand that and I totally agree and it's a mistake that gets made frequently. It's easy to impute downstream side effects or benefits to mirror assured identity and it's a mistake. We got into that in Direct a number of times in the early discussions of possession of a provider ID meant you were a good doctor kind of thinking. It's obviously not the case.

Mike Davis – VA
When you have a small scale system it's not a problem. Usually it's the right thing to do. But when you're trying to make something that needs to scale to large, you have to separate.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes. So I think we're challenged with the authentication problem right now. And even there we still have the issue, we in the aggregate will have the issue of what is the minimum level of identity proofing, identity assurance, to embed in these certificates for them to be trusted for these various purposes of identity establishment as we cross network boundaries in healthcare.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
But if you look at criteria for the class two and three, those are the criteria that are more applicable to organizations and servers.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Right, yes, we're getting ahead of ourselves to get to it as individuals, but we know we're going to eventually be asked to go there.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, but others have been there.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
Yes, and organizations too, right?

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, organizations are class 2 certificates.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
But people have figured that out as well.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, exactly.

David McCallie – Cerner Corporation – Vice President of Medical Informatics
It's how much proof of you being an organization is required?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I'm going to have to cut off, I apologize, because I think we only have about half an hour more and we do have another presentation from the NW-HIN Exchange project. So I want to try to move us along and leave some time for questions as well for the NW-HIN presenters. Why don't we go to that presentation, and we have a number of people that are probably going to be talking. I think on this slide we have Rich, Kevin, as well as Eric, so I'm going to turn it to you all and you have about 20 minutes, let's say, and we can leave a few minutes for questions at the end and a couple of minutes for next steps, so take it away.

Rich Kernan – Deloitte Consulting – Health IT Specialist
I'll get it kicked off and then kick things over to Kevin and Eric and we'll try to stay safely within the 20 minute time frame. I want to give you a general overview of the scenario in which certificates are used within the exchange, just to set the stage. Then it sounds like in addition to a discussion of the standards I think one of the topics you guys will focus on is what are the more operational aspects behind the use of the standard. So we can talk about some of the lessons learned from the operations within the NW-HIN Exchange, and Eric Heflin is going to touch on some of the technical aspects of specifying the use of those standards and some of the lessons learned there. So if we can go on to the next slide, that would be great.

Quickly, just for some background, the exchange is currently comprised of health information organizations such as state HIEs and federal agencies, IDNs, etc., and those HIOs act as nodes on a network and collectively they form the NHIN exchange, as we call it. Those nodes are connected to each other via the Internet. The HIOs do a couple of things. Number one is they act as networks in and of themselves so providers and provider systems connect to each other from within those networks by some means and some sort of standards and specifications which are outside the scope of the NHN Exchange. Finally, those nodes also, through the use of what we call gateway services or NHN Exchange gateway services, enable users who are connected to those nodes to take advantage of and use the NHN Exchange services to reach out across the Internet and then apply the NHN Exchange specifications to connect with other nodes.

So again, the technical specifications, security included they cover the communication between nodes only. They don't extend at all to cover the provider or other edge systems connections to the nodes themselves. So I think you'll hear a running theme whether it this specification or other NHIN specifications is that the specs themselves are often complicated and difficult in some cases to implement, but often our use of them is as simple as possible. In this example is that we have security requirements which govern node to node communications but don't extend beyond those nodes. So there's an overall trust fabric. It's important to remember that it's comprised of technical, certainly, specifications which we'll go in here in a minute but as well as legal and policy safeguards. Again, the technical components primarily extend only to the nodes themselves and then beyond those nodes at least within the exchange it's a policy and legal components such as DURSA, HIPAA, and other policies or legislation which govern security there.

So, I'll give you a little bit of basics of the use of certificates within the exchange. As I think many of you know, that the exchange is Web service based and … fundamental method of activity is SOAP over HTTP and the use of Web services. The messaging platform specification adopts the WSI basic profile, which describes all those sort of fundamental connectivity specifications and the WSI security profile, which covers security. I won't go through the individual profiles here but if you look in note section beneath that slide, you'll see all of the other standards and specifications or profiles, which are pulled into through the adoption of that security profile. But among them are—it's in my notes, the X.508 token profile, a typo—X.509 token profiles as well as AS basic and PKI.

So again, you have individual providers who are connected to nodes. They use the Web serves offered by their nodes to connect to other nodes. It's really important that node A and node B, when they mediate an information exchange, meets would authenticate each other and then create a secure channel between them and to encrypt the information between those nodes. Again, that's a secure channel that encryption, that authentication, only happens between the two nodes and not between node and edge system.

The next slide on ... are the basis for authentication between those nodes and then public … infrastructure is used as an encrypted and secure the channel. The ONC has contracted out to Entrust as a common certificate of authority. So there's a single root CA, an Entrust certificate, for from which the individual ones issued to NHIN participants are derived. It's a single trusted party to each transaction, which made things fairly convenient. At least for the initial stages of NHIN where you anticipated dozens or maybe even up to 100 or more nodes … single CA and this type of approach which is just fine. If we got to the point where the use cases required connectivity to individual providers or to a much smaller provider entities and you've got thousands of different nodes, it maybe a different story. But as I mentioned earlier that the use of the most standard and specifications within the exchange is simplified in some cases by constraints on the use cases.

M
Just to clarify this is the NHIN—the NWHIN exchange pilot contract?

Rich Kernan – Deloitte Consulting – Health IT Specialist
Right. The pilot really concluded in the end of 2009. Throughout 2010, the production specifications have been out there and used to varying degrees primarily by SSA and MedVirginia, now a little more in pilot by CDC and CMS and a couple of state health information exchanges. But we're in with very limited still but production mode.

M
But my question was with the contract to Entrust and the single CA, that covers the scope of the pilot and the contractors follow on to the pilot rather than potentially future use of the Gateways.

Rich Kernan – Deloitte Consulting – Health IT Specialist
Well, future use up to—and Eric jump in if you need to, but—up to several hundred or at least to different participants. So it could cover the next couple of years.

M
It's a policy decision that will apply to any use. Is that a regulatory or a policy decision, it would apply to anyone who wants to participate in the NWHIN, is it will all go through a single CA?

Rich Kernan – Deloitte Consulting – Health IT Specialist
Yes, that's the current that's specified in the spec itself right now and it's more of a—yes, it's probably more of a governance decision and it's just reflected in the technical specification. But those are the current constraints we're under right now.

M

Yes, I don't think the NHIN exchange has—the decision to go with the single CA was a decision to get things moving. It wasn't a this is the only thing that will ever happen in the future.

Eric Heflin – Director of Standards and Interoperability
Yes, that's correct. It was a pragmatic choice for now just to keep things headed in a viable implementation direction. It's also consistent with the DURSA as well.

M
That was the answer of my question we had numerous debates in Direct as to whether this was the easiest route to go is just to designate a single cert authority. It had vocal pushed backed that was not the right way to go. So I was surprised to hear that that was the way you guys did it.

Eric Heflin – Director of Standards and Interoperability
Well, the use of it probably is different between … I think there's probably ... doesn't seem right and easiest. When putting this in place for—it wasn't in place for the pilot, at least not with Entrust. It was in place when we started in production, as Rich had mentioned. Again, as John and everyone has kind of alluded it was closely aligned with the DURSA as the DURSA exists now and was reflected in the specifications as they exist now. If there does becomes a decision that we go to a multiple CA type of capability then it would require ... changes probably in the DURSA in the specs, but there's nothing technically. I mean it wasn't so much that this is a technical—just sort of technical decision, as is, this was the easiest ... with having goals of what the NHIN was approaching at that point in time.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
I have a quick question too. So this is node to node—so let's say HIO to HIO—using the Gateway. If they say inside an HIO they use a different CA for some of their end nodes and one of those end nodes is trying to read someone across the Gateway on another HIO. How would that certificate exchange happen from the end node to the HIO central point, I guess, and then through the Gateway between the HIO and the other HIO.

Eric Heflin – Director of Standards and Interoperability
The actual use case you described if I understand it correctly is that there would be a second certificate or really certification authority issuing the certificate to use with the NHIO, is that what you're asking?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Yes, exactly, if ....

Eric Heflin – Director of Standards and Interoperability
Sure. Yes, so what happens is basically most protocol stacks would have rejected it immediately. So, if that participant is tempted to use a certificate for NWHIN exchange that was not issued by the authorized CA, in this case Entrust, then basically the other end of exchange will automatically fail to validate the authenticity of the certificate for as being a trusted certificate and we reject the dialogue. So the TLS negotiation would fail. That negotiation happens on both sides. Both participants within an NWHIN exchange mutually authenticate against the same trusted entity which is the Entrust Root CA.

Rich Kernan – Deloitte Consulting – Health IT Specialist
Walter, it sounds like you might have been also asking though that beyond that node to node certificate exchange what if there's a source certificate from edge system from node A, if you will. There's no opportunity at least right now to have any sort of end to end certificate exchange. It's only at the node to node. So, as far as I know Eric there's no way to pass through if there were sort of a second certificate.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Okay, I see. Alright.

M

Yes … end to end.

M
So there is a theoretical. But one of the main differences is that this is an operational environment. So there's been choices made on the what is acceptable as an operational characteristic. That's kind of getting back to David's question about the difference between NHIN Direct where there was a lot of negatives about choosing a single authority for all of Direct versus the NHIN exchange where choosing a single authority for all NHIN exchange. The difference there again is also because the Direct Project was a specification writing project not an operational project. So there was no way to stand up a certificate authority in the Direct case.

M
There was a policy belief that it was not a good idea as well. I mean, there was both practical and theoretical. But these are policy decisions not technology constraints—

M
Yes, and I'll kind of put Mike's presentation up in the middle that is proof that we can make the technology do all of these different things that we're talking about. When you start a pilot like NHIN exchange and you have a small scope and you're only doing point to point using TLS to create a very tight knit, virtually secured network, you can take some short cuts to begin with and look to PKI's maturity as assurance that you will be able to scale upwards.

M
Yes and I wanted to make sure that there wasn't a technical reason why they had to have a single cert authority because that would go against everything else we've heard. I just want to make sure I wasn't missing them.

Eric Heflin – Director of Standards and Interoperability
It fully supported our primary use case at the time, which still is actually is a valid use case today for the NWHIN. The Direct Project has a very different use case as well too and so that's why the security Entrust model is substantially different.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
We should probably let you to continue and try to finish the—

Rich Kernan – Deloitte Consulting – Health IT Specialist
Thanks Walter. Just remember this is when—even the previous group of leadership at ONC was focused on this network of network where the way to reach providers was through focal points, which were anticipated to be health information exchanges or rather large HIOs, so a relatively huge number of nodes. Certain requirements on what those nodes have to do to authenticate and manage security of their own end users and the use of SAML to pass that information as to when node A tries to communicate with node B. The NHIN certificate immediates that authentication and SAML provide node B with the information as to how node A authenticated its own user. But it's not though the use of PKI or certificates. It's all ... via SAML.

M
Got it.

Rich Kernan – Deloitte Consulting – Health IT Specialist
So again, as part of the services we get from Entrust or our managed PKI and infrastructure solution, Kevin can touch more into this but the vendor provided solution is used to issue and revoke certificates. There are services which offer certificate revocation list checking and online certificate status protocol. When a node receives a request from another node on the NWHIN, it checks with Entrust periodically to validate that that certificate is still currently—hasn't been revoked. It checks—

M
… using a protocol or is that a—

Rich Kernan – Deloitte Consulting – Health IT Specialist
It checks against a certificate revocation list and/or the online certificate service protocol. For right now, ONC is paying for the cost of the certificates, which I forget is somewhere in the less than $500 range, if I remember. Of course, the one we selected Entrust is cross-certified to the federal bridge, which are one of their requirements for dealing with federal agencies.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
So everybody on the exchange has a single entry point into their organization? That's a question—does everyone these—these are organizational type certificates and not service certificates?

Rich Kernan – Deloitte Consulting – Health IT Specialist
That's correct, right Eric? Is … issue to each Gateway?

Eric Heflin – Director of Standards and Interoperability
Yes, one key point that I wanted to make later on too, is that the idea of the class of certificates is not, to my knowledge, part of a standard. That's actually a vendor definition and a vendor driven distinction. The actually expression of the purpose of a certificate is essentially up to the associate operational policy and implementation and use of that certificate. ... can be ignored.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I knew that the class structure was developed by VeriSign, but I thought it had been adopted widely, I think it has, as a de facto-type standard not a … type standard.

Eric Heflin – Director of Standards and Interoperability
Exactly it is a de facto standard but largely it's not necessarily something that's enforceable or enforced by stacks. But something that one could choose to look at as an additional attribute when making policy determinations but it doesn't have to be .... I would actually think that using a class code might be a bit of a distraction.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Actually, that's not the crux of my question anyway. My question really is, does one organization get one certificate or one certificate per entry point?

Eric Heflin – Director of Standards and Interoperability
Currently.

M
… service endpoint. These are service end point certificates. Now, it just happens that an organization probably only has one service end point.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Really? Because certainly—and if Arien's still around—the Direct Project certainly doesn't assume that there's only one service end point per organization, but I guess—

M
The architectures are very different though. The NHIN exchange architecture is an architecture by which you are doing queries and retrieves from your electronic medical record, or health record in your institution, into the exchange, whereas the Direct Project is pushing from one individual to another individual. So characteristically, they're going to be many to many in the case of the Direct Project and it's

going to be more of a star architecture in the case of the exchange. It's ... world but generally speaking, those are two very different architectures.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Yes, and we don't have … NHIN … either. I mean in the Direct Project doesn't have a Gateway but the exchange has multiple. So, it's one per Gateway.

Eric Heflin – Director of Standards and Interoperability
Currently that is correct. But it doesn't necessarily have to be that way for future implementations.

Rich Kernan – Deloitte Consulting – Health IT Specialist
So with that Kevin, I'll shift to you in a second. But this is a reminder so the use case is signed to the NHIN by ... back when it was I'm a physician and I'm trying to seek information that I don't currently have on a given patient. Where I think the Direct assignment was sort of the flip side of that. I'm a physician and I have information which I want to push out to a known provider.

Kevin, why don't you take away the process step if you will.

Kevin Stein
Sure. I just laid out kind of some of the steps that an organization goes through to actually get a cert. I won't read through all of it in detail but basically, there's a whole thing with the NWHIN on boarding process, which is the process that a participant goes through to basically validate that. It had implemented the specifications in a way that will allow them a successful exchange with other NWHIN participants. As part of that, they go through the actions of getting sort of a digital cert for their Gateway.

As you can see with this, it's kind of a multi-step process. As a part of the onboarding, we grant them access to the Entrust enrollment system. They then generate a certificate … request, which they then upload to the Entrust enrollment system, from there the Entrust then generates a … that they download back. In addition, they download the root and cross certificates and this provides the trust chain that was mentioned earlier. Since we are using a single common CA, all of the certificates, it will pass back up to that common root. They then go in and once they have installed or once they've downloaded all of these certs, they now go in and install them in what various implementation stacks they might have. So, we call it lessons learned here in a minute. What we found is this is where things can get complicated and where organizations can tend to struggle.

Then finally we do this twice as part of the NWHIN onboarding, you have a validation processes which I just mentioned which is where you go through various testing of regimen. Then once you've been approved to go onto the production NWHIN exchange as a full member to the exchange with other members you go through the same steps to retrieve another certificate for what is then your production system. When we looked at other CA providers of NPKI systems, they all had kind of the same set of instructions or the same set of steps that you would go through to issue the certs to the individual organizations. Are there any questions on that? If not, great. We'll go onto the next slide.

Lessons learned: One of the things I think Dave or Mike had kind of mentioned this, and John also is digital certificate basis are not widely understood. It's proven to be a challenge with multiple organizations with regards to kind of the very basic, what is a digital certificate? How do I use it? How is it created? In addition, there's complexity when you talk about ... certificate on different stacks. For instance, we've run into a case with one of—this same organization that was installing onto Windows 2003 servers. They ran into all these issues because there were like five patches that they needed to have applied that they didn't.

So, again, it really is a struggle that we're finding for a lot of organization in implementing what at least at a kind of 50,000 foot level should be a pretty simple thing, sure. It's just 509 search. I just install them. They work. Yes, but especially when you're talking kind of the Gateway to Gateway, server to server type

of communication, there are a lot of variables that tend to trip up a lot of the organizations. What we've had to do from the operations side at ONC is kind of actively help each of these organizations that become onboard in the mechanics of getting their certificates, understanding how to get the certificates, installing them, making sure all the pieces are there, in place and operating properly. So, we've had to … come up with a very detailed instructions for different implementation stack. Those that are using a Java stack versus those that are using Windows stack versus those using different application servers.

Then lastly, it's required from hands-on work usually in most cases. They will think they have everything installed. They will try to go through the validation testing process and the handshake doesn't work. So then we have to go into kind of a debugging section with them to figure out why the handshake didn't work. Maybe it was because, again, they didn't build the certificate chain correctly. Maybe it was because something at the OS level, the patch wasn't put in place. So it has been more and more complicated and time consuming aspect of the whole new NWHIN onboarding for participants in just getting this kind of basic—what we've normally had considered a very basic thing done, but the lesson learned is that it's not that basic.

Any questions on that? Okay. Next slide, then.

Eric Heflin – Director of Standards and Interoperability
I apologize for this back ground noise. I'm actually sitting in the airport in Toronto. Hopefully, am I understandable okay?

M
Yes.

Eric Heflin – Director of Standards and Interoperability
Okay great. So just very briefly, lessons learned from the specification side of things. So Kevin really spoke to the operational side of things. So my talk is just going to be what we do better from the spec side. So, from the NWHIN as far as the specifications, one, is we definitely underspecified them. There's a number optional attributes, file formats, encoding, which key value pairs within the certificate, level assurance, and as Dixie said earlier, I really want to reemphasize that point. The weakness, though, is not in certificates, it's actually in the use of certificates, it's the policy. It's the procedure … specifications. Those are really the problem areas where use of X.509 kicks in. The certificates themselves are actually really well thought out and can work really well. So again, the problems you're having I think largely because NHIN under specified some of the aspects of the certificates.

Two, some of the challenges we're facing that Kevin just talked about are a direct result of under specifying, even the test teams are having challenges because of this. For example, what's a valid organization name within a certificate? Some entities are putting in values of tests as opposed to creating an organization name. So things like that can be tightened outside … any of future use of certificates. Be very careful, go through attribute to attribute, make sure the certificates are very tightly specified. Also work with the policy people at the same time to make sure that policy equal and technology you have a large intersection.

Number three, this may be not well known, but certificates are not all the same, for example, identicrypting. Some commercial vendors will basically issue a certificate almost anonymously. You don't have to even really identify yourself or prove that you are who you say you are. Some CA's are actually very rigorous … approach will require in person identification. So identicrypting varies widely. Revocation policies and latency associated with detecting revoked certificate …. In one case, NWHIN was considering a revocation period of near real-time. We found out that the market and the vendors in the marketplace do not support a revocation of more than generally a day or two, and so—a few minutes—so vendor support is very important to understand.

Four, policy issues: We actually had considered perform or revocation. At one point, the policy … the revocation checking should be done every time the certificate was used. But when we drill down to vendors, we actually found is that most of them even to ones who used the more advanced OCSP protocol, generally only supported revocations of a day or two. As far how frequently the notification could be made between the time the certificate is revoked until really the consumers of that certificate could be aware of the fact that that has been revoked.

In addition, we've also found, one lesson learned, is please make sure that the policy people, the technical people, the test teams, and operation people all come together and have a chance to mutually review the specifications together. That would avoid a lot of iteration we face NHIN. For example, we have situations where a policy would come down, we would actually look .... From a technical perspective and specification perspective, we'd find it was perhaps not implementable exactly as is. That had to be sent back up a couple of times until we actually got it right. Then the testing team would get a hold of it and say, "Whoa, we can't test this." So if all those teams come together at least periodically to make sure there's a good intersection between policy and technology and testability and requirements, it's probable will make it a much more viable solution.

Number five, Mitch I'll just briefly mention that one thing that we've found is that it's possible for multiple keys be needed per participant. For example, this organization they needed one key for the Gateway. Also, they need another key for signing things. Another key for internal users as well too, or keys for internal users. So, a one key solution may not be sufficient. So one thing they almost got—this was actually the fact we would have to issue multiple keys for NWHIN purposes, one again, for the channel and one for other uses such as signing documents.

On six, vendor support is very wide. There are a lot options that one vendor may support that another vendor does not support. So vendor support definitely should be taken into account in terms of the realities of what exist today. ... actually exist and they have been implemented in the past and they have been deprecated. We found some OCSP options for example were implemented by a vendor and then a few years they actually deprecated that implementation. That vendor happened to be one of the co-authors of original specification.

Number seven, the certificates overall though I want to emphasize, it has been successful for us. It hasn't been perfect. It hasn't been … easy, but overall the use of certificates has actually done what we intended to set out which was at a high degree of assurance of both parties of a transaction that the other party was who they said they were.

So a few things that we're anticipating, basically gaps or anticipated things that—where things are coming down the pipeline for us that we need to address: One is the way to support cloud based gateways whereby which one gateway proxies for multiple organizations. I actually happen to be working for a vendor that it has that specific use case in mind. Where we have a cloud that my vendor would stand up for NHIN and then behind it will be a multiple states, multiple IDM's, multiple ... and so on.

Two, the problems we've seen before in the prior slide actually on the backlog for being addressed through the specification process. So this is ... and the fix is actually in the pipeline for this. Three, certificates absolutely can be used for more complex trust models than NHIN is currently using. For example, the Direct Project, that's really a Web of trust and that can be accommodated. One very practical way of doing that, in my opinion, is to have a cross science certificates whereby which you have multiple trusted roots. So the … process for Direct Project it could be for example that first you have to have to a certificate from one of the trust anchors, and then you're a trusted entity and can exchange on the Direct Project gateway.

Then organizational trust models are very different the end user trust models, point number four. For the NHIN we actually, generally we pass user information back and forth for logging and auditing and kind of ... purposes. But that information is generally not used for anything as far as policy determination. I

suspect that that's probably going to be very different compared to other projects. All the policy of determinations decision making that NHIN participant currently use today generally is based on a gateway and then some similar attributes such as the purpose of use. So end user trust model is currently not deployed for the NHIN gateway networks.

Five, one big lesson I think we've learned and Kevin really underscored this point is educational materials really need to be graded. So as those that are participating in exchange they have something to refer back to for those specific situation. Here is how you could use this certificate for your exact situation, for example.

Number six, is really a more of a philosophical issue, which is that one of the reasons we only use it ... Roots CA for the NHIN is we thought even though that was simple that it still would be challenging enough for us to do and it actually has been the case. So my advice would be when using the certificates, try to err on the side of having it simpler type of exchange, initially, and then build on that an additionally use cases have sponsors and have a need be deploy the marketplace. Again, certificates absolutely can work. They've been very viable for us and I think using them overall has been the right decision.

That's it. I'll pause for questions.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Thank you very much. I know we're running out of time. I don't know if there's maybe one question that we can entertain if anybody wants to just make a specific point before we—

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
I'd like to thank our presenters and I think that we are already over so we really should open this to the public at this point.

Judy Sparrow – Office of the National Coordinator – Executive Director
Do you want to do the public now?

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Sure. Go ahead Judy.

Judy Sparrow – Office of the National Coordinator – Executive Director
Operator, can you check and see if anybody wishes to make a comment?

Operator
We do not have any comments at this time.

Judy Sparrow – Office of the National Coordinator – Executive Director
Okay. Thank you operator.

Walter Suarez – Institute HIPAA/HIT Education & Research – Pres. & CEO
Judy, before we close I just want to make a point. There were two additional slides that we didn't cover. I added a couple of points to begin to think about guidelines and evaluation criteria. We didn't get to those but we will get to those at the next call and probably in between, just exchange some e-mail messages about those. One of them actually is a reflection on the criteria used during the HITSP, the health information technology standards panel, ... the criteria that was used by his ...HITSP to evaluate standards and recommend center. So I just wanted to make a point about the couple of slides that we didn't get to and that we would use in the next call.

I think we can close off the call. I thank you everyone for joining. Thank you very much to our speakers again and we look forward to our next call which is scheduled for February 28th. Thank you.

Judy Sparrow – Office of the National Coordinator – Executive Director
Correct.

Dixie Baker – Science Applications Intl. Corp. – CTO, Health & Life Sciences
Thank you. Bye.

Judy Sparrow – Office of the National Coordinator – Executive Director
Bye.